Gestions des services standards

Abdelali SAIDI

abdelali.saidi@gmail.com

Plan

Plan

Les fichiers journaux

Présentation

- Garder des traces des événements qui affectent les processus
- Généralement, les journaux sont placés dans le répertoire /var/log/
- La plus part des logs sont générés par le démon syslogd

Exemples de logs importants

cron, mail, messages, auth, dmesg

La configuration

/etc/syslog.conf

- La configuration se fait sur le fichier /etc/syslog.conf
- Les messages de logs sont divisés en groupes
- Dans chaque groupe, ils sont classés par priorité

La configuration

Les groupes

- auth et authpriv : authentification
- cron : messages de l'utilitaire cron
- kern : messages du noyau
- mail : le système de courrier
- user : les processus utilisateurs

Les priorités

Dans un ordre croissant, les priorités sont : emerg, alert, crit, err, warning, notice, info, debug.

La configuration

Syntaxe

Chaque ligne de configuration contient une liste de groupes de messages avec la priorité correspondante et le nom du fichier journal destination:

- groupe1.priorité1 ; groupe2.priorité2 ; ... /var/log/fichier_journal
- la priorité doit etre comprise comme priorité minimale
- la destination peut etre un fichier local comme elle peut etre un serveur distant (@serveur)

Exemple

```
authpriv.*    /var/log/secure
mail.*        /var/log/mail.log
cron.*        /var/log/cron
news.=crit    /var/log/news/news.crit
news.=err     /var/log/news/news.err
news.notice   /var/log/news/news.notice
```

La rotation des logs

Objectif

La rotation des logs est une procédure automatisée dont le but est d'archiver les anciens fichiers de journalisation.

Le mécanisme

- Typiquement, un nouveau fichier journal est créé périodiquement
- L'ancien fichier journal est renommé en lui ajoutant un suffixe "0"
- À chaque fois qu'un nouveau fichier journal est créé, on incrémente le nombre qui se trouvent dans les noms des anciens logs
- À un suffixe seuil, le fichier de journalisation peut être supprimé ou bien archivé quelque part

Remarque: il est également possible de compresser ces fichiers

La rotation des logs

Environnement de configuration

- L'outil logrotate
- Le fichier de configuration /etc/logrotate.conf
- Un fichier spécifique pour chaque service dans le répertoire /etc/logrotate.d/ (à inclure dans le fichier de configuration)

La rotation des logs

/etc/logrotate.conf

```
# faire la rotation chaque semaine
weekly
# garder les 4 dernier fichiers
rotate 4
# envoyer les erreurs à root
errors root
# après la rotation créer le nouveau fichier de log
create
# compresser les fichiers sauvegardés
compress
# inclure les fichiers de /etc/logrotate.d
include /etc/logrotate.d
# configuration des logs de lastlog et utmp
/var/log/wtmp {
monthly
    create 0664 root utmp
    rotate 1
}
```

Plan

Présentation

Le super-service

- The extended Internet services daemon
- Il gère l'utilisation des services réseau
- Il englobe des options de configuration spécifique très utiles (contrôle d'accès, journalisation, redirection, ...)

Présentation

Le fichier /etc/xinetd.conf

- Le fichier /etc/xinetd.conf est le fichier de configuration maître.
- Ce fichier doit inclure les fichiers se trouvant sur le répertoire /etc/xinetd.d (includedir /etc/xinetd.d)

Le répertoire /etc/xinetd.d

- La configuration des services est déportée dans des fichiers situés dans le répertoire /etc/xinetd.d/
- Ce répertoire comprend un fichier de configuration par service géré par xinetd.
- Le fichier porte le nom du service

Fichiers de configuration

/etc/xinetd.conf

Présentation

- Il contient des paramètres de configuration généraux
- Il n'est lu que lors du lancement du service xinetd
- Il est nécessaire de le redémarrer pour la prise en compte des modifications

Exemple

```
defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}
includedir /etc/xinetd.d
```

Fichiers de configuration

/etc/xinetd.conf

Explication

- instances : détermine le nombre maximum de requêtes qu'un service xinetd peut gérer à un moment donné
- log_type : indique à xinetd d'utiliser le journal authpriv qui enregistre des entrées de journalisation dans le fichier /var/log/auth
- log_on_success : Configure xinetd de façon à ce qu'il journalise si la connexion est établie avec succès
- log_on_failure : Configure xinetd de façon à ce qu'il journalise si la connexion échoue ou si elle n'est pas autorisée
- Configure xinetd de manière à n'autoriser que 25 connexions par seconde à un service donné. Si cette limite est atteinte, le service est retiré pendant 30 secondes

Fichiers de configuration

/etc/xinetd.d/

Présentation

- Il contient les fichiers de configuration des services
- Ces fichiers portent un nom faisant référence au service

Exemple

Le fichier /etc/xinetd.d/telnet

```
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = yes
}
```

Fichiers de configuration

/etc/xinetd.d/

Explication

- service : Définit le nom du service
- flags : Définit tout attribut pour la connexion, parmi la variété disponible. REUSE donne l'instruction à xinetd de réutiliser le support pour une connexion Telnet
- socket_type : Spécifie le connecteur réseau comme étant de type stream
- wait : Détermine si le service est mono-fils ('single-threaded', yes) ou multi-fils ('multi-threaded', no)
- user : Détermine l'ID d'utilisateur sous lequel le processus sera exécuté
- server : Définit le fichier binaire exécutable à lancer
- nice : Détermine le niveau de priorité du serveur
- disable : Détermine si le service est actif ou non

Modification des fichiers de configuration

Options de journalisation

Ces options sont utilisables aussi bien pour le fichier de configuration générale que pour les fichiers de configuration spécifiques:

- ATTEMPT : Enregistre une tentative qui a échoué
- DURATION : Enregistre la durée d'utilisation du service
- EXIT : Enregistre le statut de sortie ou le signal de fin d'un service
- HOST : Enregistre l'adresse IP de l'hôte distant
- PID : Enregistre l'ID de processus du serveur recevant la requête
- RECORD : Enregistre des informations sur le système distant dans le cas où le service ne peut pas être démarré
- ...

Modification des fichiers de configuration

Options de contrôle d'accès

Les options

Les options suivantes d'accès des hôtes sont prises en charge par xinetd :

- only_from : Permet seulement aux hôtes spécifiés d'utiliser le service
- no_access : Empêche les hôtes spécifiés d'utiliser le service
- access_times : Spécifie la fourchette de temps pendant laquelle un service particulier peut être utilisé (HH:MM-HH:MM)

Modification des fichiers de configuration

Options de contrôle d'accès

Exemple

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        no_access       = 10.0.1.0/24
        log_on_success  += PID HOST EXIT
        access_times    = 09:45-16:15
}
```

⇒ Toute tentative de connexion depuis le réseau 10.0.1.0/24 sera bloquée et enregistrée dans /var/log/auth

Modification des fichiers de configuration

Options de liaison et redirection

Xinetd prend en charge la liaison du service à une adresse IP et la redirection de requêtes entrantes pour ce service vers une autre adresse IP, nom d'hôte, ou port.

Modification des fichiers de configuration

Options de liaison et redirection

Liaison

- La liaison est contrôlée par l'option bind
- Elle lie un service donné à une adresse IP dans le système
- Cela est utile pour les systèmes ayant de multiples adresses
- Alors, seules les requêtes provenant de la bonne interface réseau seront prises en charge par le service concerné

Modification des fichiers de configuration

Options de liaison et redirection

Redirection

- Elle permet de configurer le service de manière à ce qu'il redirige toute requête pour ce service vers l'hôte et le numéro de port spécifié

Exemple

```
service telnet
{
        socket_type  = stream
        wait    = no
        server    = /usr/sbin/in.telnetd
        log_on_success  += DURATION USERID
        log_on_failure  += USERID
        bind                    = 123.123.123.123
        redirect                = 10.0.1.13 21 23
}
```

Modification des fichiers de configuration

Options de gestion de ressources

Les options

Ces options permettent d'ajouter un niveau de sécurité élémentaire contre les attaques de types déni de service (DoS)

- per_source : Détermine le nombre maximum d'instances d'un service spécifique pour une adresse IP d'origine particulière
- cps : Détermine le nombre maximum de connexions par seconde
- max_load : Définit le seuil d'utilisation d'un processeur (CPU) pour un service